NIST FRAMEWORK : Long Branch Public Schools has aligned itself with the NIST Framework and works consciously and continuously to check and recheck the integrity of our network.

IDENTIFY : Long Branch Public Schools has policies (as evidence supports through the submitted documentation for Active Directory, Google, and user agreements) that address the use of school owned technology, internet safety and use, logins, district resources, protection of privacy, and retention of data.

PROTECT : Long Branch Public Schools is outfitted with a team of network professionals that assure the integrity of our network and data. With the deployment of 2 Cisco Firewalls that are fully patched and maintained by a Certified Cisco Network Professional and the deployment of 2 clustered, for high availability, McAfee Web Gateways, our network team also uses things such as…

- Network Policies to assure account security (passwords, access, etc.)
- Website Categorization to assure no inappropriate or harmful sites are visited
- Symantec Endpoint on all of our devices with network and threat protection enabled
- Microsoft Update Server to assure all Windows based clients are fully patched with the latest updates
- PDQ Deploy to send package updates to non Windows based programs
- VLANing to streamline and segment data
- Wireshark to follow data paths and detect abnormalities
- MRTG to monitor bandwidth all the way down to a single port level
- NAGIOS to monitor the functionality and health of equipment
- Guest Networks that assure full segmentation from our network with passwords and authentication that expire daily
- Web Reporter to summarize web activity
- Note : We currently do not support any BYOD initiative and do not allow staff or students to join any personal devices to our network for reasons beyond technology limitations or security. Our district administration has made it a point to provide near endless resources to everyone who attends our schools. They have made it clear they want every student and staff member to be on the same page and have the same benefits of highly functional and always available equipment.

DETECT : With the use of aforementioned tools, our network is monitored on a daily basis by the network team with live automated alerts notifying several people whenever an abnormality occurs. Our Firewalls, Web Gateways, and Nagios monitoring system run 24/7/365 with live monitoring and real time reporting to a team of employees.

RESPOND : Our monitoring systems are setup with live time reporting of any issues. The alerts that are generated real time are sent out via text message and email to our Network Team, Head of Technical Services, and Technology Director. An active group chat is required to always be open with all of the identified members on both stationary and mobile devices which allows for instant communication. With everyone having remote connection from anywhere via a Cisco secure VPN and 2 staff members within minutes, any alert can be dealt with at any time. If a

physical problem has surfaced, all members are capable of servicing all of our equipment. If a software issue has surfaced, the person most suited for the issue on hand takes point and others assist as needed.

RECOVER : In the event of a catastrophic failure of equipment or a full contamination of a virus/cybersecurity attack, appropriate measures are taken. Running a virtual environment with backup servers in other sites, live virtual machines that have been corrupted can be shut down immediately, a fresh base image which is always patched and ready for deployment can be spun up and data can be retrieved through our backup system Commvault, which retains full and incremental backups of snapshots and data for a month. In the event of physical damage, hot spare servers can be turned on with data once again being recovered from CommVault – mitigating downtime or having to rebuild/fix entire systems.

As Long Branch Public Schools has met or exceeded the criteria, in accordance with the information presented above, we currently fall into the Tier 4 categorization of the NIST Framework. Labeled as "Adaptive" – Long Branch Public Schools has shown readiness and resiliency in all facets identified. Our network team attends seminars on network security and we have assets that are a part of the district staff, as well as outside personnel, that provide live updates from government alerts when cyber security risks reach a high level. With policies in place, physical and software protection at the forefront, live monitoring happening all of the time, recovery methods in place, and an identified budget to support each area every year, Long Branch Public Schools has assured the integrity of its network with the ability to recovery from an array of failures or breaches.